Math 126 Lecture 2

Group homomorphisms

Definition of a homomorphism.

Let G and H be groups a map

$$f: G \longrightarrow H$$

is called a **homomorphism** if

$$f(ab) = f(a)f(b)$$

for all elements a and b of G.

For example, if G=Gl(n,k) and H is the multiplicative group of non-zero elements of k then the map det which sends each matrix **a** in G into its determinant is a homomorphism from G to H. We will next study a less obvious homomorphism.

The homomorphism from SU(2) to SO(3).

Write the real three vector $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ as the two by two traceless self adjoint matrix

$$\begin{pmatrix} z & x-iy \\ x+iy & -z \end{pmatrix}.$$

This gives a 1-1 linear map between $\mathbb{R}^3$ and the set of 2×2 traceless s.a. matrices. Notice that

$$\det \begin{pmatrix} z & x-iy \\ x+iy & -z \end{pmatrix} = -(x^2+y^2+z^2).$$

If U is unitary and M is self adjoint then $UMU^* = UMU^{-1}$ is self-adjoint and has the same determinant and trace as M. Also $(UV)M(UV)^* = U(VMV^*)U^*$.

This defines a homomorphism from $U(2)$ to $O(3)$. Restrict this to $SU(2)$.

We will show that this map ϕ is a 2 to 1 map from *SU(2)* to *SO(3)*.

Rotations about the z and y axes.

Let

$U_\theta := \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix}$. Then

$$U_\theta \begin{pmatrix} z & x-iy \\ x+iy & -z \end{pmatrix} U_\theta^* = \begin{pmatrix} z & e^{-2i\theta}(x-iy) \\ e^{2i\theta}(x+iy) & -z \end{pmatrix}.$$

So $\phi(U_\theta)$ is rotation through 2θ about the z-axis. Let

$$V_\phi := \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}$$

Computation shows $\phi(V_\phi)$ is rotation through 2ϕ about the y-axis. Since every element of $SU(2)$ is conjugate to an element of the form U_θ the image of the image of ϕ lies in $SO(3)$.

The kernel.

The kernel of a homomorphism f: G $\longrightarrow$ H is the set of all elements of G which are mapped to the identity element of H. We shall show that the kernel of our homomorphism from SU(2) $\longrightarrow$ SO(3) consists of I and -I.

If U is in the kernel of ϕ then $UMU^{-1} = M$ so $UM = MU$ for every M. If we take $M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ then $MU = UM$ implies that U is diagonal and hence of the form U_θ. If we take $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ we see that $\theta = 0$ or π. So the kernel of ϕ consists of I and $-I$.

Using a theorem of Euler to show that our homomorphism maps onto all of *SO(3)*.

To show that ϕ is onto we call on a theorem of Euler which says that every element of $SO(3)$ can be written as

$$R = R^z_\theta R^y_\phi R^z_\psi$$

i.e. a rotation about the z-axis followed by a rotation about the y-axis followed by another rotation about the z-axis. Since every rotation about the y or z axis is in the image of ϕ this implies that all of $SO(3)$ is in the image. We will prove

Euler's theorem after we develop some important concepts.

The action of a group on a set, the isotropy subgroup of a point.

The action of a group G on a set M is a homomorphism from G to S_M. Equivalently, it is a map $G \times M \to M$ sending $(a, m) \mapsto am$ such that

$$em = m \quad \forall m \in M \quad \text{and } (ab)m = a(bm).$$

Let $m \in M$. The set of all $a \in G$ such that $am = m$ is a subgroup of G called the **isotropy group** of m and denoted by G_m. The concept of an isotropy group gives a precise mathematical definition to the idea of the "symmetry" of an object.

We have

$$G_{bm} = bG_m b^{-1}$$

meaning that $c \in G_{bm}$ if and only if $c = bab^{-1}$ for some $a \in G_m$.

Proof of Euler's theorem about rotations.

Let M be the unit sphere and $G = SO(3)$. Let n denote the north pole. Any $R \in SO(3)$ is determined by Rn and the image of any unit vector tangent to M at n. So if B is any other element of $SO(3)$ with $Bn = Rn$, we can arrange that the unit vector is in the right direction by rotating about the axis through Bn, In other words,

$$R = CB, \quad C \in SO(3)_{Bn}.$$

Now we can get to any point on the unit sphere from the north pole by first rotating about the y-axis to achieve the correct latitude, and then rotating about the z-axis to achieve the correct longitude. In other words we can choose

$$B = R^z_{\theta} R^y_{\phi}.$$

So $C = BR^z_{\psi}B^{-1}$ for some ψ and so

$$R = CB = BR^z_{\psi}B^{-1}B = BR^z_{\psi} = R^z_{\theta}R^y_{\phi}R^z_{\psi}$$

proving Euler's theorem.

Action induced on subsets and on functions.

If G acts on M, it also acts on 2^M, the set of all subsets of M by

$$aS := \{as | s \in S\}.$$

It also acts on the set of all functions on M by

$$(af)(m) := f(a^{-1}m).$$

If f is a function which takes on only two values, say 0 and 1, this action generalizes the action on 2^M,

Orbits.

Let G act on M and let $m \in M$. The **orbit through** m denoted by $G \cdot m$ is the set of all points of the form am, $a \in G$.

2.3.1 $\#G = \#(G \cdot m) \times \#G_m$ and some consequences.

If S is a finite set we let $\#S$ denote the cardinality of S. Suppose G is finite and acts on M. If $m \in M$ and $n \in G \cdot m$, then $n = am$ for some $a \in G$. If also $n = bm$, then $b^{-1}a \in G_m$, and conversely. So there are exactly $\#G_m$ elements a such that $am = n$, and so $G \cdot m$ partitions G into $\#(G \cdot m)$ cosets each having $\#G_m$ elements, proving the formula in the title of this subsection. In particular both $\#G \cdot m$ and $\#G_m$ divide $\#G$.

Applications of

$$\#G = \#(G \cdot m) \times \#G_m$$

- G acts on itself by left multiplication, and hence acts on 2^G, the set of all subsets of G. Under this action, if H is a subgroup, then the isotropy group of H is exactly H. hence we conclude that

  $$\#H \text{ divides } \#G$$

  for any subgroup of G.

- We can apply this to the subgroup H generated by single element a. Then $\#H$ is the smallest positive integer n such that $a^n = e$. This is called the **order** of a. We see that the order of any element must divide $\#G$. This is a theorem of Lagrange.

- A group G is called a p-group (where p is a prime) if $\#G$ is a power of p. This implies that every $\#G \cdot m$ is a power of p. The set of **fixed points** of G (for any group action) is the set of all $m \in M$ such that $am = m$ for all $a \in G$. It is denoted by $\mathrm{Fix}(G, M)$ or $\mathrm{Fix}(G)$ if M is understood. The orbit through a point m of $\mathrm{Fix}(G)$ consists of the single point $\{m\}$. If G is a p-group, all other orbits O have the property that $\#O$ is divisible by

More Applications: The Sylow theorems.

Let G be a finite group and write $\#G = p^n k$ where k is not divisible by p. A subgroup of G of order p^n is called a p-**Sylow subgroup** . There are four statements (due to Sylow) concerning Sylow subgroups.

Sylow subgroups exist.

The number of Sylow subgroups is $\equiv 1 \bmod p$.

The number of Sylow subgroups divides # G

All Sylow subgroups are conjugate.

Ludwig Sylow 1832 - 1918

Lemma 1.1 *Let p be a prime and k an integer not divisible by p. The number of ways of selecting a subset with p^n elements from a set with $p^n k$ elements is congruent to k mod p.*

Proof of lemma. The number in question is the coefficient of x^{p^n} in

$$(1+x)^{p^n k} = \left((1+x)^{p^n}\right)^k.$$

But $(1+x)^{p^n} \cong 1 + x^{p^n} \bmod p$. And the coefficient of $x^{p^n k}$ in $(1+x^{p^n})^k$ is k. □

Proof of the existence of Sylow subgroups. Let M consist of the set of all subsets of G of cardinality p^n. G acts on M by virtue of its left multiplication action on itself. Decompose M into orbits. Not every orbit O has the property that $\#O$ is divisible by p for then $\#M$ would be divisible by p contrary to the lemma. Let O be an orbit for which $\#O$ is not divisible by p. So $O = G \cdot S$ where S is a subset of G such that

$$\#S = p^n \quad \text{and} \quad \#G_S = \#G/\#G \cdot S = tp^n.$$

We would be done if we could show that $t = 1$.

We have shown that there is a subset S of G such that

$$\#S = p^n \quad \text{and} \quad \#G_S = \#G/\#G \cdot S = tp^n.$$

Now $G_S s \subset S$ for any $s \in S$ so the coset $G_S s \subset S$. But multiplication on the right by s is a one to one map on G, and hence

$$\#G_S = \#(G_S s) \leq \#S = p^n.$$

So $t = 1$ in the above expression and $\#G_S = p^n$ and hence G_S is a p-Sylow subgroup. $\square$

Notice that the above proof shows that the S we have chosen has the property that $G_S s = S$ for any $s \in S$, and hence $s^{-1} G_S s$ is a Sylow subgroup in the orbit $O = G \cdot S$ and so $s^{-1} G_S s = s^{-1} S$. So O is the orbit of the Sylow subgroup $s^{-1} G_S s$, and the isotropy subgroup of $s^{-1} G_S s$ is just itself. So $\#O = k$, and every orbit whose cardinality is not divisible by p has exactly k elements and exactly one point of this orbit is a Sylow subgroup. No orbit whose cardinality is divisible by p can contain a Sylow subgroup.

every orbit whose cardinality is not divisible by p has exactly k elements and exactly one point of this orbit is a Sylow subgroup. No orbit whose cardinality is divisible by p can contain a Sylow subgroup. So the number N_p of Sylow subgroups is the same as the number of orbits whose cardinality is not divisible by p and each such orbit has cardinality k. In particular, since we can partition M into orbits,

$$\#M \equiv kN_p \mod p.$$

We have proved that $\#M \equiv kN_p \mod p$. On the other hand, the lemma says that $\#M \equiv k \mod p$. So $N_p \equiv 1 \mod p$. $\square$

We have proved the second assertion:

$$N_p \equiv 1 \ \mathbf{mod}\ p.$$

Let P be a p-Sylow subgroup of G and let Q be a p-subgroup of G (which eans that $\#Q = p^m$ for some $m \leq n$). The third Sylow theorem says that

Q is contained in a conjugate of P.

This implies that any two Sylow subgroups are conjugate.

Let P be a p-Sylow subgroup of G and let Q be a p-subgroup of G

We want to prove that

Q is contained in a conjugate of P.

For this we will need two lemmas. The first is a general lemma about two subgroups of a group. Let A and B be subgroups of a group G. We let AB denote the set of all elements of G which can be written as ab with $a \in A$ and $b \in B$. So AB is a subset of G, but need not be a subgroup. But $A \cap B$ *is* a subgroup.

Lemma 1.2 $\#(AB) = (\#A)(\#B)/\#(A \cap B)$.

Proof. We know that $A \cap B$ is a subgroup of A. Let

$$x_1(A \cap B),\ x_2(A \cap B), \ldots x_r(A \cap B)$$

be the distinct cosets of $A \cap B$ in A. So every element of A is in one of these cosets. Also, if $i \neq j$ then $x_j x_i^{-1} \notin A \cap B$. Let $ab \in AB$. Write $a = x_i g$ for some i with $g \in A \cap B$. So $ab = x_i gb \in x_i B$. Also, the cosets $x_i B$ are disjoint, for if not $x_i B = x_j B$ for some $i \neq j$ implying that $x_i^{-1} x_j \in A \cap B$ which is not the case. So

$$\#(A)/\#(A \cap B) = \#(AB)/\#B$$

which is equivalent to the statement of the lemma. $\square$

For the second lemma we need some notation. If B is a subgroup of any group G, then $N_G(B)$ denotes the isotropy subgroup of B under the conjugation action, i.e. the set of all $a \in G$ such that $aBa^{-1} = A$. If A is a subgroup of $N_G(B)$ then AB is a subgroup.

Lemma 1.3 *Let P be a p-Sylow subgroup of a group G. Then any p-subgroup Q of $N_G(P)$ is contained in P. In particular, P is the unique p-Sylow subgroup of $N_G(P)$.*

Proof. Suppose that $\#Q = p^m$. Then QP is a subgroup of order p^{n+m-s} where $\#P = p^n$ and $\#(Q \cap P) = p^s$ by the preceding lemma. Since p^n is the largest p-th power dividing $\#G$, we must have $m \leq s$. On the other hand, $P \cap Q$ is a subgroup of Q, and hence $s \leq m$. so $s = m$ and hence $P \cap Q = Q$ which says that $Q \subset P$. $\square$

Lemma 1.3 *Let P be a p-Sylow subgroup of a group G. Then any p-subgroup Q of $N_G(P)$ is contained in P. In particular, P is the unique p-Sylow subgroup of $N_G(P)$.*

Proof of the assertion. Let M denote the set of distinct G-conjugates of P. Let P act on M by conjugation. So $P \in \mathrm{Fix}(P, M)$. We claim that P is the only element of $\mathrm{Fix}(P, M)$. Suppose that $gPg^{-1} \in \mathrm{Fix}(P, M)$. This says that

$$x(gPg^{-1})x^{-1} = gPg^{-1}, \quad \forall\ x \in P$$

or

$$(g^{-1}xg)P(g^{-1}xg)^{-1} = P$$

so $(g^{-1}xg) \in N_G(P)$. This is true for all $x \in P$ so $g^{-1}Pg \subset N_G(P)$ and since $\#((g^{-1}Pg) = \#P$ the preceding lemma implies that $g^{-1}Pg = P$. So there is only one fixed point and hence $\#M \equiv 1 \bmod p$. Now consider the conjugation action of Q on M. Since $\#M \equiv \#\,\mathrm{Fix}(Q, M) \bmod p$ we conclude that $\mathrm{Fix}(Q, M) \neq \emptyset$. So there is a $g \in G$ such that

$$x(gPg^{-1})x^{-1} \quad \forall\ x \in Q$$

so $g^{-1}Qg \subset N_G(P)$ and hence $g^{-1}Qg \subset P$, again by the last lemma, so $Q \subset gPg^{-1}$. $\square$

In particular, any two p-Sylow subgroups are conjugate.

The number of p-Sylow subgroups divides $\#G$.

Indeed, the number of p-Sylow subgroups is the number of elements in the single orbit of the conjugacy action of G on the set of p- Sylow subgroups since we know that all such are conjugate. But we know that the number of elements in an orbit of any G action divides $\#G$. $\square$